

(12) UK Patent Application (19) GB (11) 2 378 865 (13) A

(43) Date of A Publication 19.02.2003

(21) Application No 0211994.9

(22) Date of Filing 24.05.2002

(30) Priority Data

(31) 0113572

(32) 04.06.2001

(33) GB

(51) INT CL⁷

H04L 9/32

(52) UK CL (Edition V)
H4P PDCSA

(56) Documents Cited

EP 0892521 A2
WO 1999/057847 A1

WO 2001/041360 A2
WO 1997/012460 A1

(71) Applicant(s)

Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto,
California 94304, United States of America

(72) Inventor(s)

Adrian Baldwin
Simon Shiu

(74) Agent and/or Address for Service

Richard Anthony Lawrence
Hewlett-Packard Limited, IP Section,
Filton Road, Stoke Gifford, BRISTOL,
BS34 8QZ, United Kingdom

(58) Field of Search
UK CL (Edition T) H4P
INT CL⁷ H04L

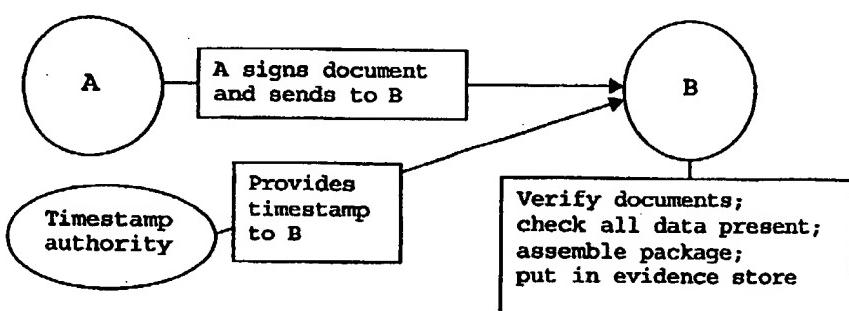
Other: ONLINE DATABASES: WPI, EPODOC, JAPIO.

(54) Abstract Title

Packaging evidence for long term validation

(57) A method of long-term validation of documents is used to verify digital signatures and time stamps even after they have expired. The method involves the formation of a complete package comprising a document (10), a digital signature (12), a public key associated with this signature (14), a timestamp (20) indicating when the document was digitally signed, and evidence of the authority of the signature (16). Further optional inclusions are a timestamp for the evidence of the authority of the signature, policy statements, Certificate Revocation Lists (CRL) and a chain of certificates up to a root authority thus providing an "evidence trail" which can be verified or authenticated simultaneously in a single step.

Figure 1.



GB 2 378 865 A

Figure 1

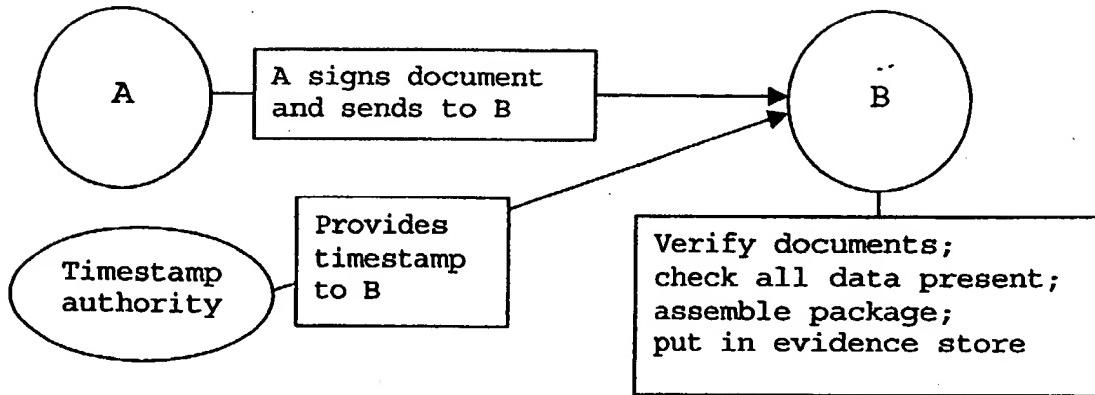
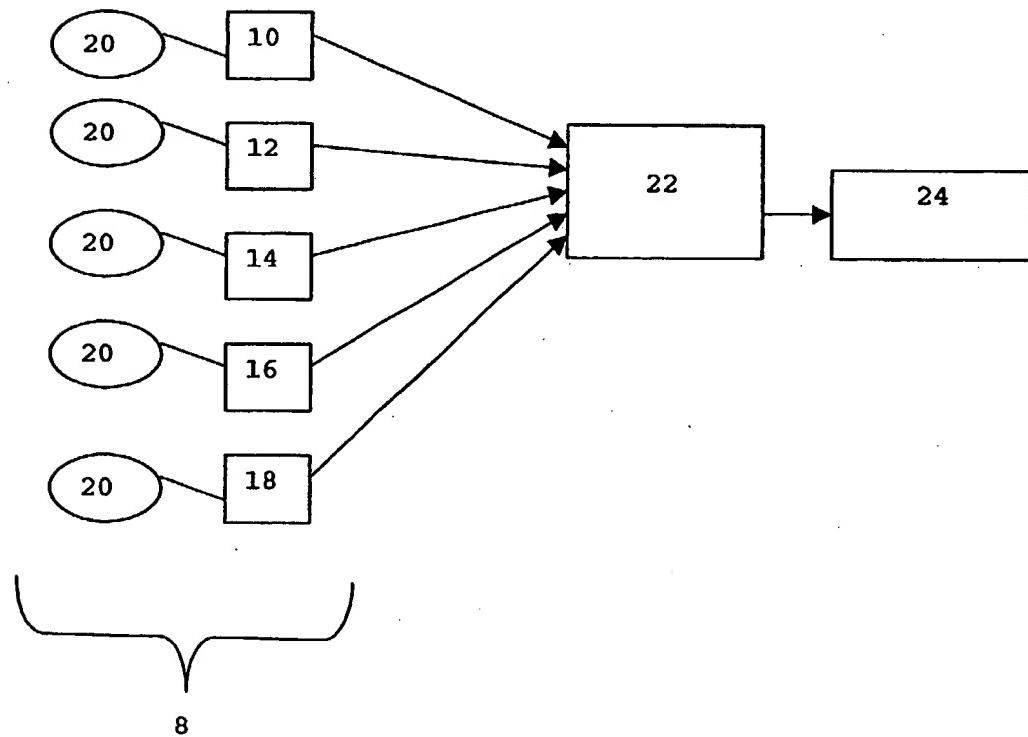


Figure 2



PACKAGING EVIDENCE FOR LONG TERM VALIDATION

This invention relates to a method of packaging digital evidence for long term validation and to a system for the
5 packaging of digital evidence for long term validation.

It is well known to make use of public key cryptography to validate digital documents as originating from a particular user having access to related public and
10 private keys. The same system can be used to allow only that user to access a document encoded with the public key. The use of public key cryptography is typically implemented by use of digital certificates. A digital certificate may be issued by a certification authority
15 (CA) which checks the credentials or personal information/financial information (whatever information is particularly relevant) before issuing a certificate to that user. The certificate may then be provided to reliers or third parties to authenticate that the user is
20 who they say they are. The relier takes it on trust that the CA has conducted whatever checks are necessary to issue the user with the certificate. Chains of certificates may be produced whereby a root CA issues a certificate to a second CA to certify that the second CA
25 is trusted by the root CA. The second CA may then issue a certificate to a third CA on the basis that the third CA is trusted by the second CA. The third CA may then issue a certificate to a user, who may use the certificate with an independent party who trusts the validity of the
30 certificate on the basis that the root authority is trusted and the relationships which the root authority keeps are also trusted.

Documents such as emails can be digitally signed by use of public key cryptography when a user encrypts a signature for an email using his private key. A third party can 5 authenticate that signature by decrypting the signature with the public key.

A problem exists of how to package and maintain a 10 digitally signed document as evidence which can be interpreted at a later date, for example in a court of law. Typically, a document retention period may be seven years, although at present a CA will not necessarily retain certification information for that period of time. 15 An existing CA called VeriSign^(R&TM) keeps different levels of certificates. VeriSign's level 2 and level 3 certificates are retained for five years. A CA such as VeriSign will only keep certification details, rather than any document which has been signed with a certificate issued by the CA. Furthermore, by making use of the reliance on the CA in 20 the way described above disadvantages are found because reliance is placed on an outside party to prove the validity and meaning of signatures at later dates.

According to a first aspect of the present invention a 25 method of packaging digital evidence from a signatory for long term validation by a relier comprises:

a third party independent from the signatory and the 30 relier assembling a package for potential subsequent validation, said package comprising:

a document for subsequent use;

a digital or electronic signature for said document;

a public key associated with the signature, for decryption thereof;

5

evidence from a certification authority (CA) of the identity or authority of the signatory of the document;

10 a time authentication for at least the document and the signature; and

evidence from a time authentication authority validating the or each time authentication;

15

the method also further comprising making the contents of the package available for verification; and

20 making the package available for storage for subsequent potential use.

The package may optionally then be verified by a fourth party, a verification client, which the relier may use to verify the package contents before storage.

25

The production of the package described advantageously produces self-contained evidence of the document having been signed by a verifiable party and at a verifiable time, for subsequent use.

30

The evidence is preferably packaged whilst a certificate covering the digital or electronic signature is valid. The method may include validation of digital evidence

after expiry of a certificate covering said digital or electronic signature. The method may include the contents of the package being verified before expiry of a certificate covering said digital or electronic signature.

5

The method advantageously allows a package to be stored for validation of a certificate covering the digital signature after expiry of the certificate. Thus, although a certificate may be valid whilst the package is assembled 10 and verified, the certificate may expire before validation is required. The fact that the package was verified during validity of the certificate is sufficient to allow validation at a later stage.

15 The time authentication may be a time stamp.

The document may be a contract or other document required to validate a transaction at a later date.

20 The evidence from the CA and/or the evidence from the time authentication authority may optionally be included in the form of a reference to a location of that evidence, said location preferably being in a data store in which the package is stored.

25

This provides the advantageous option that a signatory and a relier wishing to store the package for subsequent potential use may negotiate over which parts of a package the relier may require to be in the package and which 30 parts may be incorporated by reference.

The evidence from a CA may include a certificate chain up to a trusted root CA. A certificate revocation list (CRL)

may also be included. A policy statement for the certificate or each certificate in the chain may also be provided.

- 5 The certificate chain thereby extends up to a trusted root CA, who the user is willing to rely on to verify the source of the certificate chain.

10 The evidence from the time authentication authority may include a chain of authorities up to a root time authentication authority. A CRL for the time authentications may also be included. A policy statement for the or each CA or time authentication authority may also be included.

15

The time authentication chain is thereby verifiable up to a trusted root time authentication authority. Also the time authentication can be verified using the policy statement, without recourse to the authority concerned.

20

The time authentication may be performed as one time authentication on the package as a whole. In this way the package is advantageously complete, given that all the evidence needed is authenticated at the same time.

25

The time authentication may be performed on the specified items in the package individually. In this way regular use of a time authentication service could allow multiple production of the required time authentications for 30 different packages, rather than having to obtain a single time authentication each time one is required.

A time authentication may also be provided for the evidence from the CA.

The package may be stored in a data store, which is
5 preferably located on a computer. The document and/or certificate is preferably in the form of a computer file.

According to a second aspect of the present invention a method of packaging digital evidence for long term
10 validation comprises:

assembling a package for subsequent validation, said packaging comprising:

15 a document for subsequent use;

a digital or electronic signature for said document;

20 a public key associated with the signature, for decryption thereof;

evidence or a reference to an address of evidence from a certification authority (CA) of the identity or authority of the signatory of the document;

25 a time authentication for at least the document and the signature;

and evidence or a reference to an address of evidence from
30 a time authentication authority validating the or each time authentication;

the method further comprising verifying the contents of the package; and

storing the package for subsequent potential use, wherein
5 the assembly of the package is carried out by a third party independent from the signatory and a relier.

According to a third aspect of the present invention apparatus for the packaging of digital evidence for long
10 term validation comprises:

a first computer programmed to assemble a package for subsequent validation, said package comprising:

15 a document for subsequent use;

a digital or electronic signature for said document;

20 a public key associated with the signature, for decryption thereof;

evidence or a reference to an address of evidence from a certification authority (CA) of the identity or authority of the signatory of the document;

25

a time authentication for at least the document and the signature;

30 and evidence or a reference to an address of evidence from a time authentication authority validating the or each time authentication; and

the apparatus further comprising a second computer programmed to verify the contents of the package; and

5 a third computer programmed to store the package for subsequent potential validation.

The first, second and/or third computers may be the same computer.

10 The apparatus may be operable to package the evidence whilst a certificate covering the digital or electronic data is valid. The apparatus may be operable to validate the digital evidence after expiry of a certificate covering the digital or electronic signature.

15 The first, second and/or third computers may be independent from each other.

20 According to a fourth aspect of the present invention a recordable medium is recorded with a computer program operable to perform the method of the first aspect.

All of the features disclosed herein may be combined with any of the above aspects, in any combination.

25 Specific embodiments of the present invention will now be described, by way of example, and with reference to the accompanying drawings in which:

30 Figure 1 is a schematic diagram showing the relationship between the signatories of a contract and the digital signing and storage thereof; and

Figure 2 is a schematic block diagram of a system for packaging evidence for long term validation

In its simplest form a method for packaging digital
5 evidence for long term validation is to form a package of
a digital document together with evidence of the authority
of a signature in the document and a time stamp indicating
when the document was digitally signed. All of these
pieces forming parts of the packaged evidence.

10

A digital time stamp is similar to a digital certificate
in that it is provided by a third party, which may be a
notary service, similar to a certification authority (CA),
which verifies the time and date and production of a
15 particular time stamp. The time stamp is encrypted with
public key cryptography, as described above. The time
stamp may have its own chain of certification to a root
time stamping authority, similar to that as described in
relation to CAs. The time stamp may alternatively be any
20 form of time authentication.

As shown in Figure 2, the package of evidence 8 will
include a document 10 for retention, a signature 12 for
the document 10, a public key 14 associated with the
25 signature (for verification of the signature), first
evidence 16 of the owner/authority associated with the
public key 14 used, second evidence 18 of the
authority/trustworthiness of a time stamping service and a
trusted time stamp 20 for each of the above from a time
30 stamping service.

All of the elements of the package 8 can then be put into an evidence store 24, which could for instance be a computer database file.

- 5 In more detail, the standard such as public-key cryptography standards #7 (PKCS #7) entitled Cryptographic Message Syntax Standard from RSA Laboratories can provide the framework for packaging signed data and is used as the underlying format for the method and system for packaging
10 evidence described herein. PKCS 7 provides a framework which has the ability to have included in it a plurality of certificates and also certificate revocation lists (CRLs) which may be deemed relevant. A CRL is a list provided by a CA to indicate which certificates issued by
15 the CA have been revoked. PKCS 7 does not have the facility for including a policy/usage statement of a certificate, as described below, to be included in the standard as it currently exists. However, suitable modifications can be made to PKCS 7 to allow for inclusion
20 of such a statement.

A package of evidence may be compiled as follows, as shown in relation to Figures 1 and 2.

- 25 A computer 22 is used to compile the package 8 by first receiving the document 10 signed by party A with his signature 12. Party B who is receiving the signed contract from A then runs a normal verification of the signature 12 by using the public key 14 which A provides
30 with the signed document 10.

B then checks that all the data required in the contract is present. This data includes the first evidence 16 of

the owner/authority associated with the key used, which, if appropriate, includes a chain of CAs to a root CA. B checks that the chain of CAs is acceptable before proceeding further. Associated with the chain of CAs is a 5 policy statement of each certificate which sets out the terms and conditions for which a particular certificate is valid. Assuming that B is prepared to accept the first evidence 16, the computer 22 then goes on to check the second evidence 18.

10

The second evidence 18 includes, where appropriate, a chain of time stamp authorities and also a policy statement from the or each time stamping authority giving details of the effectiveness parameters of the 15 verification of the time stamp given.

The various pieces of the package 8 are then assembled into a single computer file or collection of computer files or similar package and then placed in an evidence 20 store 24, which in this example is a computer database.

Various modifications of the method and system described above are possible where there is some level of trust between A, the signatory of the document 10, and B, the 25 party wishing to retain the document 10 as evidence.

Firstly, a third party notary service may be used to provide the necessary time stamping and packaging of the evidence on behalf of the signer A and the relier B. This 30 time stamping and packaging is conducted for B and the package 8, having been verified and collated, is provided to B for storage by B. Alternatively, a notary service, potentially independent from the above mentioned notary

service, may also provide storage of the evidence package 8.

The subsequent validation procedure is straightforward.

- 5 The package is retrieved from the evidence store 24 and essentially the same steps carried out as are carried out in the verification step: the digital signature on the document is tested with the public key and the evidence of the associated CA is considered, and the timestamping evidence and the evidence of the associated timestamping authority is considered. The document is retrieved and validated if the digital signature and the timestamping evidence are considered satisfactory.
- 10
- 15 A further alternative would be to use the method and system described above in two parts. A may provide the signed document together with whatever information B requires such as time stamping and change of authority. B's decision on what information is required could be based on information which B already has in its evidence store 24.
- 20

For example, if B has evidence of a chain of authority already in its evidence store 24 which is identical to 25 that of a new package of evidence 8 then he may decline that extra information in order to reduce his storage requirements. Such an example may be used where a lot of business is conducted between A and B. If this method is used, then it may be possible for B to reduce storage 30 requirements for evidence by up to 80 or 90%. Consequently, there would be significant benefits achieved by arranging to have a negotiation procedure between A and B to set out what time stamping and authentication

information is required. Once the negotiation has been conducted, then A can provide B with whatever B has specified. B would then package the information provided by A, together with references to other pieces of evidence 5 in its evidence store 24 which, in this instance, validate what has been received on trust from A. B then places the reduced information package into its evidence store 24.

A further option would be in the situation where B trusts 10 documents provided by A and he trusts A's time stamp, then A could produce and send a package to B for B to then check and store. In this situation, the time stamping authority used may provide to A all the authorities and chains of authority required for A to simply pass this on 15 to B, B having taken on trust that the time stamping authority used by A is acceptable.

A modification of the negotiation procedure discussed above would be that party A simply provides all the 20 various parts of the package 8 discussed above and sends the evidence package 8 to B for verification, which B can then check before storing in his evidence store 24.

The time stamping of the package 8 could either be 25 conducted on each of the elements of the package or could be carried out on the package 8 as a whole. This issue is a completeness versus efficiency issue. Time stamping the whole package 8 provides completeness, because all the evidence is validated at the same time. However, if the 30 same signature and/or time stamping service is regularly used, it will be more efficient to regularly create time stamps of the authority of the signature and the time stamp, with the ability to be able to produce these in

association with the evidence package 8. The latter is more time efficient, but could be more open to a lack of trust between parties not familiar with each other's method of working.

5

Legitimately signed policy statements and certificates and time stamping certificates are included in the package (which is itself time stamped) because verification of the certificates and time stamps at a much later date is 10 allowed by this method without recourse to the issuing service (e.g. CA) itself. Consequently, the fact that additional information is stored is disadvantageous, but the advantage of not needing to revert to the issuing service has considerable advantages for long term storage 15 of evidence, because the issuing authority may have changed or be untraceable at a later date when verification of the evidence is required.

It will be appreciated that the packaging and verification 20 steps are carried out in embodiments by appropriately programmed computers. A suitable computer program for programming appropriate computers to carry out these steps may be provided to an appropriate computer by data carrier or any other appropriate means.

25

The method of packaging and system for packaging described above has significant advantages over previous methods and systems, because a single evidence package can itself be used to determine and provide evidence of when the package 30 was signed and also to authenticate the signatures and time of signature for the package. Consequently, it is not necessary to have recourse to outside parties to validate the evidence. Also, the party wishing to retain

the evidence has control of that evidence and so less reliance needs to be made on outside parties, unless a user wishes to put reliance on an outside party, at his discretion.

CLAIMS:

1. A method of packaging digital evidence from a signatory for long term validation by a relier comprises:

5

a third party independent from the signatory and the relier assembling a package for potential subsequent validation, said package comprising:

10 a document for subsequent use;

a digital or electronic signature for said document;

15 a public key associated with the signature, for decryption thereof;

evidence from a certification authority (CA) of the identity or authority of the signatory of the document;

20

a time authentication for at least the document and the signature; and

25 evidence from a time authentication authority validating the or each time authentication;

the method also further comprising making the contents of the package available for verification; and

30 making the package available for storage for subsequent potential use.

2. A method as claimed in claim 1, in which the evidence is packaged whilst a certificate covering said digital or electronic signature is valid.
- 5 3. A method as claimed in claim 1 or claim 2, in which the time authentication is a time stamp.
- 10 4. A method as claimed in any preceding claim, in which the evidence from the CA and/or evidence from the time authentication authority is included in the form of a reference to a location of that evidence.
- 15 5. A method as claimed in claim 4, in which the location of the evidence is in a data store in which the package is to be stored.
- 20 6. A method as claimed in any preceding claim, in which the evidence from the CA includes a certificate chain up to a trusted root CA.
7. A method as claimed in any preceding claim, in which a certificate revocation list (CRL) is also included in the package.
- 25 8. A method as claimed in any preceding claim, in which a policy statement for the or each certificate is also provided in the package.
- 30 9. A method as claimed in any preceding claim, in which the evidence from the time authentication authority includes a chain of authorities up to a root time authentication authority.

10. A method as claimed in any preceding claim, in which a CRL for the time authentications is also included in the package.
- 5 11. A method as claimed in any preceding claim, in which a policy statement for the or each CA or time authentication authority is also included in the package.
- 10 12. A method as claimed in any preceding claim, in which the time authentication is performed as one time authentication on the package as a whole.
- 15 13. A method as claimed in any preceding claim, in which the time authentication is performed on the specified items in the package individually.
- 20 14. A method as claimed in any preceding claim, in which a time authentication is also provided for the evidence from the CA.
15. A method as claimed in any preceding claim, further comprising verifying the contents of the package.
- 25 16. A method as claimed in claim 15, in which the package is verified by a fourth party, a verification client, which the relier uses to verify the package contents before storage.
- 30 17. A method as claimed in claim 15 or claim 16, in which the contents of the package are verified before expiry of a certificate covering said digital or electronic signature.

18. A method as claimed in any preceding claim, further comprising storing the package for subsequent potential use.
- 5 19. A method as claimed in claim 18, in which the package is stored in a data store.
20. A method of using a document with an associated digital signature after expiry of the digital signature,
- 10 comprising:
- retrieving from storage a package assembled for subsequent validation, said package comprising: a document for subsequent use; a digital signature for said document; a public key associated with the signature, for decryption
- 15 thereof; evidence from a certification authority of the identity or authority of the signatory of the document; a time authentication for at least the document and the signature; and evidence from a time authentication authority validating the or each time authentication;
- 20 validating the package without reference to the certification authority; and
- using the document.
21. Apparatus for the packaging of digital evidence
- 25 comprises:
- a first computer programmed to assemble a package for subsequent validation, said package comprising:
- 30 a document for subsequent use;
- a digital or electronic signature for said document;

a public key associated with the signature, for decryption thereof;

5 evidence or a reference to an address of evidence from a certification authority (CA) of the identity or authority of the signatory of the document;

a time authentication for at least the document and the signature; and

10

and evidence or a reference to an address of evidence from a time authentication authority validating the or each time authentication;

15

wherein the first computer is adapted to make the contents of the package available for verification, and to make the package available for storage.

20

22. Apparatus as claimed in claim 21, further comprising a second computer programmed to verify the contents of the package.

25

23. Apparatus as claimed in claim 22, further comprising a third computer programmed to store the package for subsequent potential validation.

24. Apparatus as claimed in claim 23, in which the first, second and/or third computers are the same computer.

30

25. Apparatus as claimed in any of claims 21 to 24, which is operable to package the evidence whilst a certificate covering said digital or electronic date is valid.

26. A recordable medium recorded with a computer program operable to perform the method according to any one of claims 1 to 17.
- 5 27. A method substantially as described herein with reference to the accompanying drawings.
28. Apparatus substantially as described herein with reference to the accompanying drawings.



Application No: GB 0211994.9
Claims searched: All

Examiner: Mark Lewney
Date of search: 12 December 2002

Patents Act 1977 : Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance	
X, P	1-6, 8-9, and 11-26.	WO01/041360A2	(EORIGINAL) - Consider whole document.
X	1-7, 9-10, 12-13, 15-19, and 21-26.	WO99/057847A1	(DOCUMENT AUTHENTICATION SYSTEMS) - Consider whole document.
X	1-6, 9, 12-13, 15-19, and 21-26.	WO97/012460A1	(DOCUMENT AUTHENTICATION SYSTEMS) - Consider whole document.
A		EP0892521A2	(HEWLETT-PACKARD) - Consider whole document.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	B	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKCT⁶:

H4P

Worldwide search of patent documents classified in the following areas of the IPC⁷:

H04L

The following online and other databases have been used in the preparation of this search report :

WPI, EPODOC, JAPIO